



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,933	10/01/2003	Richard H. Boivie	YOR920030398US1 (8728-647)	9603
46069 7590 02/08/2008 F. CHAU & ASSOCIATES, LLC 130 WOODBURY ROAD WOODBURY, NY 11797			EXAMINER ALMEIDA, DEVIN E	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 02/08/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/677,933

Applicant(s)

BOIVIE ET AL.

Examiner

Devin Almeida

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 November 2007.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 11,13,14,16-19 and 22-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,13,14,16-19 and 22-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

This action is in response to the papers filed 11/28/2007.

Response to Arguments

Applicant's arguments with respect to claims 11, 22 and 23 have been considered but are not persuasive. Sudia teach preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key in paragraph 0249 i.e. In an instance of third party upgrade, the manufacturer could sign a firmware upgrade certificate containing a public key of the third party firmware provider and issue it to that third party. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto. Upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device and then issue a "process third party firmware upgrade" instruction. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture. If both signatures verify, the upgrade is accepted and the device performs the desired upgrade).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 11, 14, 16, 18 and 22-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudia (U.S. 2001/0050990). With respect to claims 11 and 22, a method for ensuring that a processor will execute only authorized code, said method comprising: reading a certificate including a first public key into a protected memory (see paragraph 0249 i.e. the manufacturer could sign a firmware upgrade certificate containing a public key of the third party firmware provider and issue it to that third party... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device); validating said certificate with a second public key permanently stored on said processor (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture); reading a signed authorized code into said protected memory (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private

signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate); and branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory upon verifying said digital signature (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

With respect to claim 13, wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 14 and 25, wherein said protected memory is physically protected (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 16 and 26, wherein the integrity of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 18, wherein the privacy of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claim 23, a computing device for securely executing authorized code, said computing device comprising: a protected memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer) for storing signed authorized code, which contains an original digital signature (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); and a processor in signal communication with said

protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in of said signed authorized code is original in accordance with first public key stored in said protect memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture) and validated by a second public key permanently stored on said processor (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate), and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

With respect to claim 24, wherein the integrity of the contents of said protected memory is protected by encryption (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 17, 19, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) in view of Morgan et al (U.S. Patent # 6,185,685). With respect to claims 17 and 27, Sudia does not teach wherein the integrity of said authorized code is protected with symmetric key encryption. Morgan teaches wherein the integrity of said authorized code is protected with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31). Morgan teaches using a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) (see Morgan column 8 line 60 - column 9 lines 31). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) to increase the security to the encryption algorithm (see Morgan

column 2 lines 32-65). Therefore one would be motivated to have encrypted the authorized code with a symmetric key before storing it in the protected memory and decrypted the authorized code with the symmetric key for execution of the authorized code.

With respect to claims 19 and 28, wherein the privacy of said authorized code is protected at run time with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to

Application/Control Number:
10/677,933
Art Unit: 2132

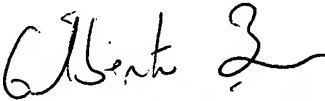
Page 9

5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to
4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA
Devin Almeida
Patent Examiner
1/5/08


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100